

Remarks

Claims 1-72 are pending in the application. Claims 1-72 are rejected. All rejections are respectfully traversed.

The invention re-authenticates and protects communication security. Using a key lease generated by performance of a primary authentication protocol, a secondary authentication protocol is performed between a client electronic system (client) and a network access point electronic system (AP). The key lease includes a key lease period for indicating a length of time in which the key lease is valid for using the secondary authentication protocol instead of the primary authentication protocol. If the secondary authentication protocol is successful, a session encryption key is generated for encrypting communication traffic between said client and said AP.

Claims 1, 12, 23, 34-36, 47-49, and 60-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Rune, (U.S. 5,850,444).

The invention authenticates devices using a first protocol and re-authenticates using a second protocol. Rune encrypts communications between terminals in a generic access network (GAN) but never authenticates devices at all. It appears that the Examiner has confused device authentication with session encryption. Rune describes encryption keys used for communication sessions on a GAN. It would be readily understood by a person of ordinary skill in the art that there is no device authentication performed in a GAN. For a better understanding of GAN communication,

the Examiner is directed to two paragraphs in Rune. The Examiner is first directed to col. 1, lines 35-40, below:

graphic location. This generic mobile radio network is referred to as the "Generic Access Network" (GAN). In order to more readily understand the present invention, which deals primarily with encrypting communications traffic between terminals and a GAN, a brief description of such a GAN is provided below with respect to FIG. 1.

40

The Examiner is further directed to col. 2, lines 54-59, below:

service networks that do not have that capability. However, since a GAN does not know the identity of its users (the service network subscribers), it must be capable of encrypting radio traffic using encryption keys that are created without knowing a subscribing terminal's identity or authenticity. Unfortunately, most existing mobile communications

It should now be readily understood that Rune has nothing to do with authentication protocols and can never anticipate the invention, which uses both primary and secondary authentication protocols.

The examiner points to col. 4, lines 16-39, where Rune describes public/private key pairs for encrypted communication between the unauthenticated devices in the GAN, see e.g., lines 33-35, below:

identity. Furthermore, since the GAN does not need to know the identity of such a terminal, the GAN is not required to maintain a database of individual terminal encryption keys.

The section has nothing to do with authentication protocols. The same is true for col. 6, lines 59-65, which describes public key expiration, and col. 5, line 54 – col. 6, line 15, which describes a key exchange in more detail. None of the above describes authentication protocols. In fact, Rune specifically describes encrypted communications between unauthenticated devices. It appears that Rune fails to teach a single element of what is claimed. For at

least the above reasons, it would be readily apparent to a person of ordinary skill in the art that Rune can never anticipate what is claimed. Therefore, the Examiner is requested to reconsider and withdraw all rejections based in Rune.

Claims 2-6, 13-17, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Dole (U.S. 6,628,786).

As stated above with respect to claims 1, 12, 23, 34-36, 47-49, and 60-62, Rune never describes device authentication at all. Dole fails to cure the defects of Rune. Dole describes a random number generation method used for encrypting communications between computers.

The Examiner's assertion that Dole teaches generating a first random number associated with said client and a second random number associated with said AP as claimed, is pure conjecture because there is never any description of associating random numbers with a computer such as a client or AP in col. 6, lines 5-27, see below:

5 Referring now to FIG. 3, a flowchart illustrating a method of implementing the present invention is presented. Normally, the method of the present invention will be implemented as a computer program ("application") residing on a host computer. However, it will be appreciated by
10 those skilled in the art that the method of the present invention may be implemented through the use of electronic hardware or through the use of a combination of hardware and software.

15 The random number generator is started with a request for random numbers (step 50). Normally, the internal state of the random number generator will have previously been set, based upon a prior operation. Next, the application will check to determine whether any additional sources of entropy have been received (step 52). Additional sources of
20 entropy may consist of prior secret session keys, nonces, private/public key pairs generated for encryption protocols such as RSA or random key values utilized to implement the Diffie-Hellman key exchange protocol. If no additional sources of entropy have been received, the application will
25 proceed to generate random numbers based on the existing internal state (step 60).

The Examiner is requested to specifically point out exactly which words above mean generating a first random number associated with said client and a second random number associated with said AP, as claimed. The applicants see only random number generation for encryption purposes. Further still, there is no teaching of primary or secondary authentication protocol, or re-authenticating.

The hashing described in Dole is for encryption of a particular message and has nothing to do with a secondary authentication protocol using a key lease from performance of a primary authentication protocol, as claimed. Regarding claims 6, 17 and 28, Rune never describes authentication protocols, as claimed. Therefore, the keys described by Rune are irrelevant to what is claimed.

Claims 7-11, 18-22, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Dole and in further view of Kessler, et al., (U.S. 6,789,147 – Kessler).

Claimed is using said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys. The section at col. 5, lines 18-27 referenced by the Examiner does not even hint at generating first and second session encryption keys based on the explicitly recited elements above, see, e.g., col. 5, lines 29-32, below:

conjunction with FIGS. 3–8. Additionally, such security operations could include, but are not limited to, a request to ³⁰
(1) generate a random number, (2) generate a prime number, (3) perform modular exponentiation, (4) perform a hash operation, (5) generate keys for encryption/decryption, (6) perform a hash-message authentication code (H-MAC) operation, (7) perform a handshake hash operation and (8) ³⁵
perform a finish/verify operation.

There is nothing above that describes the explicitly claimed combination of elements to generate the first and second session keys, as claimed.

The same is true for the claimed applying a HMAC-MDS algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key. There is no description of applying HMAC-MDS algorithm to the particular

concatenation to produce either a first or second session key as recited in the claims. The Examiner is also reminded that the invention re-authenticates using a second authentication protocol and a key lease from a primary authentication protocol. No such thing is ever considered by Rune, Dole, or Kessler.

Claims 37, 50, and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Kennelly et al., (U.S. 6,754,702 – Kennelly).

As stated above Rune fails to teach authenticating using a primary authentication protocol and re-authenticating using a secondary authentication protocol, as claimed. Kennelly fails to cure that defect. Further, Kennelly applies user attribute information to determine authorization levels during a session. This has nothing to do with the claimed authentication. The invention uses context information to determine a length of tie a key lease is valid during the secondary authentication protocol. Kennally is useless for making the invention obvious.

Claims 38-43, 51-56, and 64-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Babu, et al., (U.S. 6,122,639 – Babu).

As stated above, Rune fails to teach primary and secondary authentication protocols for authenticating and re-authenticating, as claimed. The Examiner's assertions that Rune teaches a key lease from performing a primary authentication protocol includes identifiers for secondary authentication protocols is simply erroneous, as discussed above.

Babu describes a change detection application used for network management in a manage information base (MIB) and is completely outside of the field of endeavor of the invention and Rune. Babu has nothing to do with either Rune or what is claimed. There is no motivation to combine those references, nor would a combination be operable for either intended purpose.

Claims 44, 57, and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Kung, et al., (U.S. 5,434,918 – Kung).

Claimed is wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on symmetric encryption. As stated above, Rune fails to teach authentication and re-authentication using primary and secondary authentication protocols, as claimed.

Kung describes a mutual authentication protocol using random numbers, user IDs and passwords to complete the mutual authentication. Kung only authenticates (mutually) using a single authentication protocol. Kung never describes authentication and re-authentication using primary and secondary authentication protocols, as claimed. Therefore, Kung fails to cure the defects of Rune and cannot be used to make the invention obvious.

Claims 45, 58, and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Burns, et al., (U.S. 6,792,424 – Burns).

Claimed is wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a one-way hash function

message authentication code (HMAC) implementation. As stated above, Rune fails to teach authentication and re-authentication using primary and secondary authentication protocols, as claimed.

Burns describes a method that authenticates and then provides authorization based on a color classification system. Again, a person of ordinary skill in the art would never confuse authentication with authorization. Burns never describes authentication and re-authentication using primary and secondary authentication protocols, as claimed. Therefore, Burns fails to cure the defects of Rune and cannot be used to make the invention obvious.

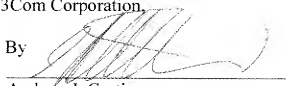
The same is true for claims 46, 59, and 72.

It is believed that this application is now in condition for allowance. A notice to this effect is respectfully requested. Should further questions arise concerning this application, the Examiner is invited to call Applicant's attorney at the number listed below.

Please charge any shortage in fees due in connection with the filing of this paper to Deposit Account 50-3650.

Respectfully submitted,
3Com Corporation,

By



Andrew J. Curtin
Attorney for the Assignee
Reg. No. 48,485

350 Campus Drive
Marlborough, MA 01752
Telephone: (508) 323-1330
Customer No. 56436